OIST OKINAWA INSTITUTE OF SCIENCE AND TECHNOLOGY GRADUATE UNIVERSITY

Lecture 3: Quantum Cryptography

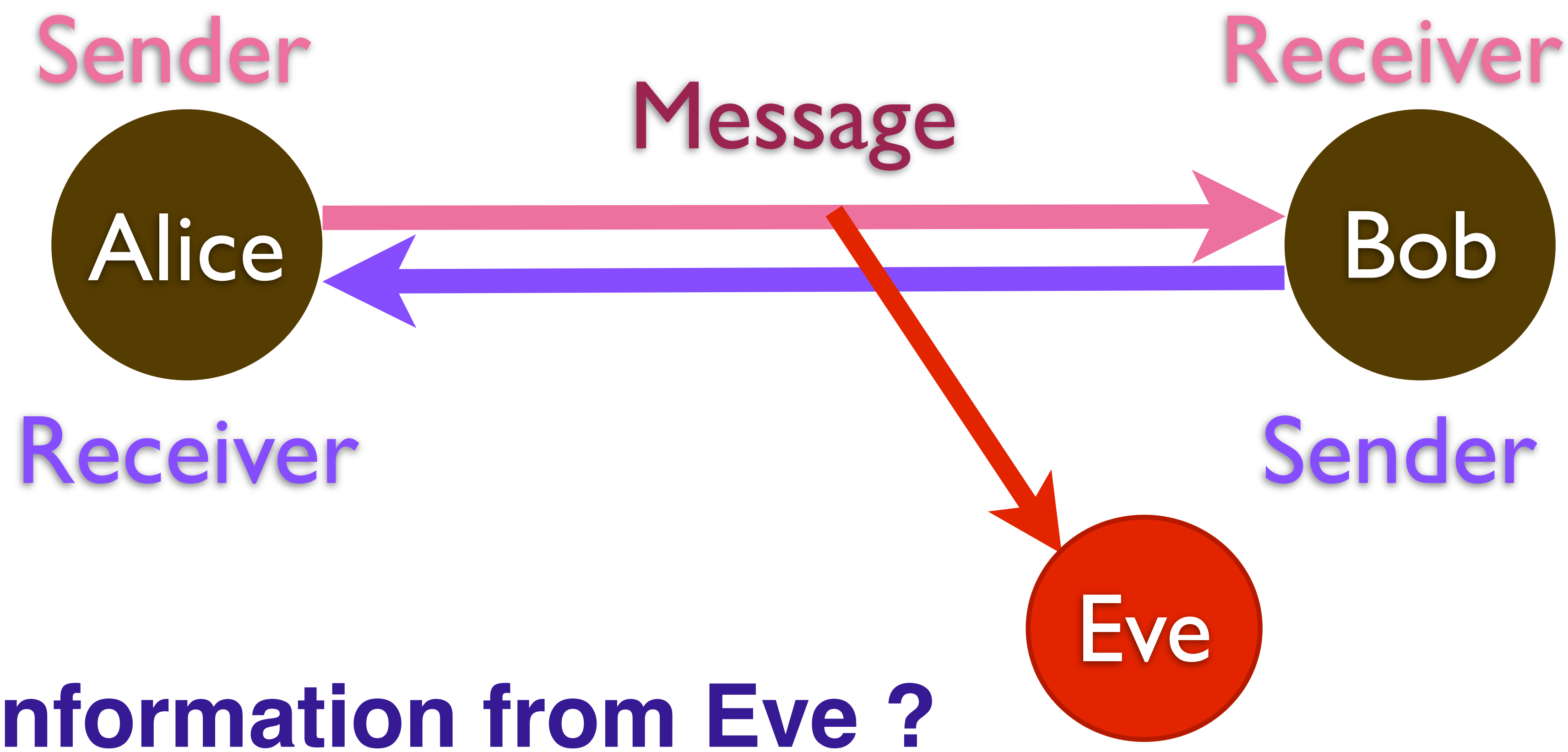
C M Chandrashekar

Communication Basics

Communication is an activity of conveying information through the exchange of thoughts, messages, or information, as by speech, visuals, signals, writing, or behavior.

Communication requires :

1. A Sender
2. A Message
3. A Recipient



How to secure information from Eve ?

How to achieve secure communication ?

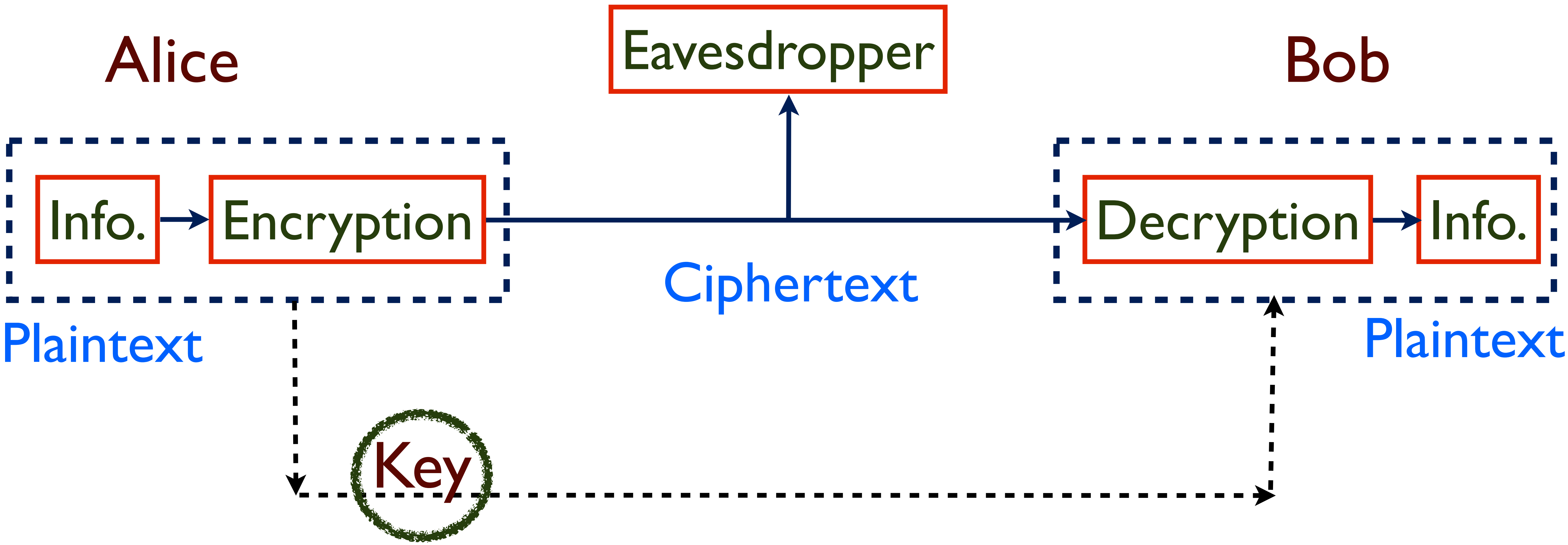
An algorithm (a *cryptosystem* or cipher) is used to combine a message with some additional information— known as the key—and produce a *cryptogram*. This technique is known as *encryption*.

For a cryptosystem to be secure, it should be impossible to unlock the cryptogram **without the key**.

Cryptography is the art of rendering a message unintelligible to any unauthorized party. It is part of the broader field of cryptology, which also includes **cryptoanalysis** - the art of code breaking.

Although confidentiality is the traditional application of cryptography, it is used nowadays to achieve broader objectives, such as authentication, digital signatures, and nonrepudiation.

A Classical Cryptographic Communication System



Cryptography Basics

Cryptosystem

Symmetric

Asymmetric

Same key for encrypt and decrypt
Key is send securely

Public key to encrypt and private key to decrypt

RSA encryption : Algorithm for public key encryption

Ron Rivest, Adi Shamir and Leonard Adleman (1978)

RSA Encryption Algorithm

Easy problem

Given two large primes p and q compute

$$n = p \times q$$

Hard problem

Given n compute p and q

Its the most widely used public key cryptography.
Algorithm is based on the presumed difficulty of factoring a product of two large primes number.

Theoretically it can be broken
Shor's algorithm can find factor for any number

One Cannot :

1. take a measurement without perturbing the system

2. determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy

3. simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis

4. draw pictures of individual quantum processes

5. duplicate an unknown quantum state

Basics

Orthonormal Basis

$$O = \{|0\rangle, |1\rangle\}$$

$$O_1 = \{|+\rangle, |-\rangle\}$$

Two set of Orthonormal basis

Each qubit can be written as : $a|0\rangle + b|1\rangle$

Other orthonormal basis : $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Quantum Key Distribution (Quantum Cryptography)

Alice and Bob need a one-way (public) quantum channel (through which they can exchange qubits) and a public (classical) channel (to send normal bits).

Alice and Bob will use the quantum channel and the classical channel to establish the key using two-stage protocol, called the BB84 protocol.

BB84 : Stage 1

Communication over a quantum channel

1. Generate the secret key to be shared only by Alice and Bob :

Alice flips a fair coin to generate a random sequence of zeros and ones (normal bits)

2. Communicating each bit :

For each bit in the random sequence, Alice flips a fair coin. If heads, she sends bit b as $|b\rangle$. If tails, she sends bit b as $|b'\rangle$.

3. Measuring qubit communicated :

Each time that Bob receives a qubit, he has no way of knowing which basis was used. He flips a fair coin to select one of the two bases, and he measures the qubit using that basis. We will see that if he guesses correctly, the measurement will correspond to the bit sent by Alice. If he guessed incorrectly, the measurement will agree with Alice in 50% of the cases.

BB84 : Stage 1 - Case analysis

If Alice sends $|0\rangle$, and Bob measures using basis O, the measurement will be 0 with probability 1.

If Alice sends $|0\rangle$, and Bob measures using basis O_1, the measurement will be 0 with probability 1/2, since:

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$

Other Cases

AS	$\vert 0\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert 0\rangle$	$\vert 1\rangle$	$\vert -\rangle$	$\vert 0\rangle$	$\vert 1\rangle$
BMB	O	O_1	O_1	O	O_1	O	O	O_1	O
BR	$\vert 0\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert 0\rangle / \vert 1\rangle$	$\vert \pm\rangle$	$\vert 1\rangle$	$\vert 0\rangle / \vert 1\rangle$	$\vert \pm\rangle$	$\vert 1\rangle$

AS : Alice sends

BMB : Bobs measuring basis

BR : Bob records

Communication over a public channel

Phase 1: raw key extraction

1. Bob communicates to Alice which basis he used for each of his measurements.

2. Alice communicates to Bob which of his measurements were made using the correct basis.

3. Both Alice and Bob discard the bits for which they used incompatible bases. The resulting bitstrings are the raw keys. If Eve has not eavesdropped, the raw keys are the same.

BB84 : Stage 1 and Stage 2 - Case analysis

Bobs measuring basis

They check results

Alice sends | Bob records | This becomes

$\|0\rangle$	O	$\|0\rangle$	✓	0
$\|+\rangle$	O_1	$\|+\rangle$	✓	0
$\|-\rangle$	O_1	$\|-\rangle$	✓	1
$\|+\rangle$	O	$\|0\rangle/\|1\rangle$	X	-
$\|0\rangle$	O_1	$\|\pm\rangle$	X	-
$\|1\rangle$	O	$\|1\rangle$	✓	1
$\|-\rangle$	O	$\|0\rangle/\|1\rangle$	X	-
$\|0\rangle$	O_1	$\|\pm\rangle$	X	-
$\|1\rangle$	O	$\|1\rangle$	✓	0

BB84 : Evil Eavesdropping Eve

What happens if Eve eavesdrops on the quantum channel? For now, let's examine opaque eavesdropping: Eve intercepts the qubit, measures it, and sends the qubit on to Bob.

Like Bob, Eve does not know which basis Alice is using. That means that with probability 1/2 she uses the wrong basis when eavesdropping.

For example, if Alice sends $|0\rangle$, and Eve eavesdrops using basis O_1, what is the probability that Eve measures 0 ?

If Eve's measurement is 0, the qubit after measurement will be |+>. Suppose Bob measures using the same basis as Alice. Then Bob's measurement will be 0 with probability 1/2. Since Bob uses the same basis as Alice, this bit will not be discarded, but it is wrong with probability 1/2.

BB84 : Stage 1 and Stage 2 - Case analysis

Alice sends	EMB	Eve records and sends	BMB	Bob records	This becomes
$\vert 0\rangle$	O	$\vert 0\rangle$	O_1	$\vert\pm\rangle$	
$\vert +\rangle$	O_1	$\vert +\rangle$	O	$\vert 0\rangle/\vert 1\rangle$	
$\vert -\rangle$	O_1	$\vert -\rangle$	O_1	$\vert -\rangle$	
$\vert +\rangle$	O	$\vert 0\rangle/\vert 1\rangle$	O_1	$\vert\pm\rangle$	
$\vert 0\rangle$	O_1	$\vert\pm\rangle$	O	$\vert 0\rangle/\vert 1\rangle$	
$\vert 1\rangle$	O	$\vert 1\rangle$	O	$\vert 1\rangle$	
$\vert -\rangle$	O	$\vert 0\rangle/\vert 1\rangle$	O_1	$\vert\pm\rangle$	
$\vert 0\rangle$	O_1	$\vert\pm\rangle$	O	$\vert 0\rangle/\vert 1\rangle$	
$\vert 1\rangle$	O	$\vert 1\rangle$	O_1	$\vert\pm\rangle$	

EMB : Eves measuring basis

BMB : Bobs measuring basis

BB84 : Stage 2 cont.

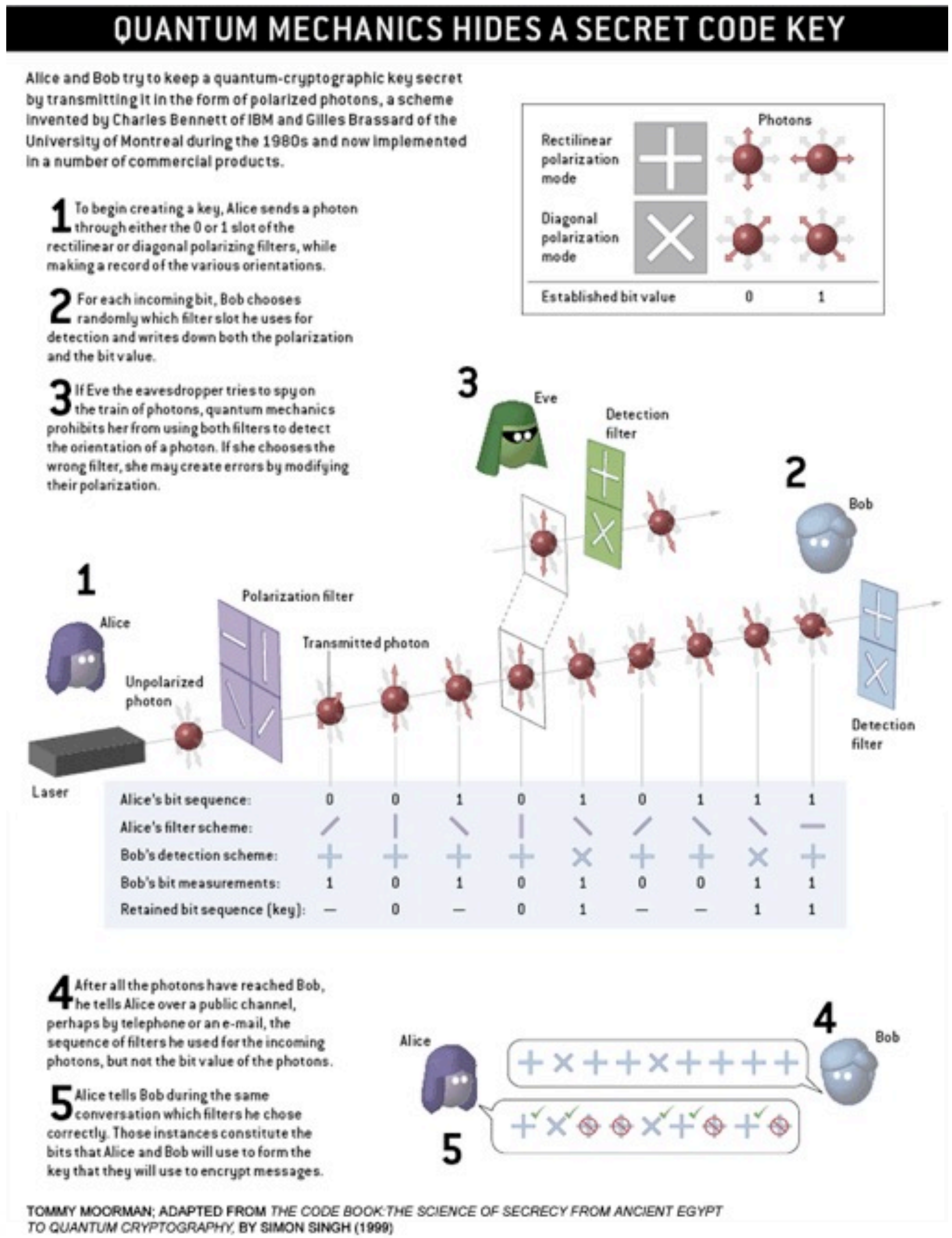
Communication over a public channel

Phase 2: error estimation

Over the public channel, Alice and Bob compare small portions of their raw keys to determine the error rate. If the error rate is grater than 0, they know that Eve has been eavesdropping. They discard the keys and start from scratch.

If the error rate is 0, they will both delete the disclosed bit from their raw keys, obtaining the final key.

Quantum Key Distribution using Photons



QUANTUM MECHANICS HIDES A SECRET CODE KEY

Alice and Bob try to keep a quantum-cryptographic key secret by transmitting it in the form of polarized photons, a scheme invented by Charles Bennett of IBM and Gilles Brassard of the University of Montreal during the 1980s and now implemented in a number of commercial products.

1 To begin creating a key, Alice sends a photon through either the 0 or 1 slot of the rectilinear or diagonal polarizing filters, while making a record of the various orientations.

2 For each incoming bit, Bob chooses randomly which filter slot he uses for detection and writes down both the polarization and the bit value.

3 If Eve the eavesdropper tries to spy on the train of photons, quantum mechanics prohibits her from using both filters to detect the orientation of a photon. If she chooses the wrong filter, she may create errors by modifying their polarization.

Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	—	0	—	0	1	—	—	1	1

4 After all the photons have reached Bob, he tells Alice over a public channel, perhaps by telephone or an e-mail, the sequence of filters he used for the incoming photons, but not the bit value of the photons.

5 Alice tells Bob during the same conversation which filters he chose correctly. Those instances constitute the bits that Alice and Bob will use to form the key that they will use to encrypt messages.

TOMMY MOORMAN; ADAPTED FROM *THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY,* BY SIMON SINGH (1999)

Air-to-ground quantum key distribution

Ludwig Maximilian University, performed the experiment at an airport near Munich using a specially-equipped plane.

BB84

September 2012